

A Conceptual Analysis of Disinformation

Don Fallis

University of Arizona

1515 East First Street

Tucson, AZ 85719

(520) 621-3565

fallis@email.arizona.edu

ABSTRACT

In this paper, the serious problem of *disinformation* is discussed. It is argued that, in order to deal with this problem, we first need to understand exactly what disinformation is. The philosophical method of conceptual analysis is described, and a conceptual analysis of disinformation is offered. Finally, how this analysis can help us to deal with the problem of disinformation is briefly discussed.

Keywords

accuracy, conceptual analysis, disinformation, epistemology, information quality, lying, misinformation, philosophy

1. INTRODUCTION

Accuracy is a critical dimension of information quality (cf. [1]). People can easily acquire false beliefs about the world as a result of inaccurate and misleading information. And such false beliefs can often lead to significant emotional, physical, and financial harm.

Inaccurate and misleading information can have such bad consequences whether the source of the information made an honest mistake (*misinformation*) or actually intended to deceive (*disinformation*).¹ But how we deal with the problem of inaccurate and misleading information *can* depend on the intentions of the source. For example, effective techniques for identifying disinformation are likely to be different from the

¹ We might hold that disinformation and misinformation are mutually exclusive categories (cf. [2], p. 134). Alternatively, we might hold that disinformation is a proper subset of misinformation. In other words, misinformation would simply be inaccurate information in general (cf. [3], p. 201). I do not take a position in this paper on the best way to analyze the concept of misinformation.

techniques that work for inaccurate and misleading information in general. Indeed, it will often be more difficult to identify disinformation since the source of the information does not want us to realize that the information is inaccurate or misleading.

Disinformation is nothing new, of course. Forged documents, doctored photographs, deceptive advertising, deliberately falsified maps, and government propaganda have been around for years. The standard example is the *disinformation campaign*, known as Operation Bodyguard, used during World War Two to hide the intended location of the D-Day invasion (cf. [4], pp. 71-75). Among other deceptions, the Allies sent out fake radio transmissions in a successful attempt to convince the Germans that there was a large force in East Anglia that was ready to attack Calais (rather than Normandy). However, disinformation has recently become a much more pressing threat to information quality.

New information technologies are making it easier for people to create and disseminate information that is intended to deceive.² For example, people are able to deceive Internet users by creating websites that “impersonate” the websites of reputable sources of information (cf. [5]). Also, people are able to convincingly manipulate visual images (cf. [6]). In fact, it now requires very little technical skill to create and widely disseminate disinformation. For example, anyone with Internet access can anonymously insert misleading information into Wikipedia (cf. [7]).

Moreover, the problem of disinformation is a critical one for information science (cf. [2], [7], p. 1665, [9], [10], [11], [12]). Libraries and other information services can easily end up being unwitting (and sometimes witting) conduits for the spread of disinformation. In addition to the disinformation that patrons may access over the Internet, many library collections include government propaganda and historical fabrications (cf. [13]). Recognizing the problem of disinformation, the American Library Association has recently issued a “Resolution on Disinformation, Media Manipulation & the Destruction of Public Information” [14].

² There was the same sort of opportunity for deception when new printing technology first made books widely available. In particular, there was often a question of whether you held in your hands the authoritative version of a given text (cf. [8], pp. 30-31). Techniques eventually developed for assuring ourselves of the authority and reliability of books. But such techniques are not always immediately available with new information technologies.

In order to deal with this threat to information quality, information scientists need to find answers to several important questions about disinformation. For example:

- Why is disinformation as prevalent as it is?
- Under what circumstances is disinformation most prevalent?
- How can we deal effectively with the problem of disinformation?
- How can disinformation be identified?
- Can the problem of disinformation be dealt with in a way that does not violate rights to free speech and intellectual freedom?

Before we can address these questions, however, we need to understand exactly what disinformation is. In other words, we need a *conceptual analysis* of disinformation.

2. THE METHOD OF CONCEPTUAL ANALYSIS

Several years ago, the information scientist Christopher Fox gave an influential conceptual analysis of *information* and *misinformation* [3]. But he did not consider disinformation. This paper will provide a conceptual analysis of disinformation and will briefly indicate how such an analysis can help us to address the aforementioned questions.

The goal of the method of conceptual analysis is to find a list of *necessary* and *jointly sufficient* conditions that correctly classify things as falling under a given concept or not (cf. [15], section 2.1). Plato famously used this method in his dialogues to try to understand such concepts as *justice*, *knowledge*, and *love*. For example, according to the “Platonic” analysis of knowledge, something is knowledge if and only if it is *justified*, *true*, and *believed*. That is, if something is knowledge, then it is justified, true, and believed (the necessity condition). Also, if something is justified, true, and believed, then it is knowledge (the sufficiency condition). In our case, we need to find a list of conditions that are necessary and jointly sufficient for something to count as disinformation.

In order to determine if such an analysis is correct, the method of conceptual analysis has us appeal to the *intuitions* of competent speakers of the language about whether particular (often hypothetical) cases fall under the given concept (cf. [3], pp. 24-25). As the philosopher of language John Austin pointed out in [16], leveraging intuitions in this way can help us to understand important phenomena in the real world. For example, to test the Platonic analysis of knowledge, we look at things that our intuition tells us are instances of knowledge and check them against the proposed conditions (i.e., are they justified, true, and believed?). Also, we look at things that satisfy the proposed conditions (i.e., things that are justified, true, and believed) and consider whether our intuition says that they are instances of knowledge (cf. [17]). In our case, we need to appeal to intuitions about whether specific pieces of information count as disinformation (given that we know certain things like whether the information is accurate, who created the information, why they created it, etc.).

Admittedly, ‘disinformation’ is a relatively new term compared with terms like ‘knowledge’ and ‘lying’. It is only about fifty

years old. As a result, the meaning of ‘disinformation’ may not be quite as fixed as the meaning of these other terms. However, we must have somewhat stable, shared intuitions about the use of the term. Otherwise, we would not be able to communicate effectively with each other using the term. Moreover, even if there is some disagreement about whether the term applies to certain cases, the method of conceptual analysis can still yield a useful taxonomy of deceptive phenomena in the vicinity of disinformation.

3. THE VARIETIES OF DISINFORMATION

Before we start trying to identify necessary and jointly sufficient conditions for disinformation, it will be useful to lay out the main varieties of disinformation with some examples.

(1) Disinformation is usually taken to be a *governmental* or *military* activity (as with Operation Bodyguard). As George Carlin put it, “the government doesn’t lie, it engages in disinformation.” In addition, the standard dictionary definition of disinformation is “deliberately misleading information announced publicly or leaked by a *government* or especially by an intelligence agency.”³ However, other organizations can also produce “deliberately misleading information.” In particular, news services are frequently sources of disinformation (cf. [4], pp. 23-53). In fact, *single individuals* are often the source of disinformation. For example, individual reporters (e.g., Jayson Blair of the *New York Times* and Janet Cooke of the *Washington Post*) have simply made up stories. Also, there have recently been some high-profile cases of purported memoirs that turned out to be fictional creations (cf. [18], [19]).

(2) Disinformation is often the product of a carefully planned and technically sophisticated deceit (as with Operation Bodyguard). For example, hackers have intentionally disseminated inaccurate information by directly modifying the websites of news services such as *Yahoo! News* and the *New York Times* (cf. [20]). However, creating disinformation can be as simple as telling a lie. For example, when President Clinton said to the American people, “I did not have sexual relations with that woman, Miss Lewinsky,” he was disinforming them. In fact, even manipulating the contents of a website does not always require sophisticated hacking skills. Anyone can purposely (and anonymously) add inaccurate information to Wikipedia. For example, the entry on the journalist John Seigenthaler was famously modified to falsely claim that he was involved in the Kennedy assassinations (cf. [7], p. 1665).

(3) Disinformation does not always come *directly* from the organization or the individual that intends to deceive. For example, news services have often been tricked into disseminating inaccurate or misleading information created by someone else. A few years ago, an investor created a fraudulent press release stating that the CEO of Emulex Corporation had just resigned (cf. [5]). When this fraudulent press release was subsequently published by several news services (including *Bloomberg*, *CBS Marketwatch*, and *Dow Jones*), Emulex stock lost over half its value in just a few hours.

³ This definition comes from the *American Heritage Dictionary of the English Language* (2006, 4th edition). The *Oxford English Dictionary* provides almost exactly the same definition.

(4) Disinformation is often written or verbal information. But other types of inaccurate information (e.g., doctored photographs) can also be disinformation (cf. [6]). For instance, Stalin and Mao each had people who had fallen out of favor removed from photographs.⁴ Also, during the Cold War, the Soviets deliberately falsified maps in an attempt to fool their enemies about where important sites were located (cf. [21], pp. 115-118).

(5) Disinformation is often distributed very widely (e.g., to anyone with a newspaper subscription, to anyone with a television, to anyone with Internet access). But disinformation can also be targeted at specific people or organizations. For example, Jeff Danzinger (of the *Los Angeles Times*) has a cartoon that shows a couple working on their taxes. The caption is “Mr. and Mrs. John Doe (not their real names) hard at work in their own little Office of Strategic Disinformation.” Such disinformation is presumably aimed directly at the *Internal Revenue Service*.

(6) The intended victim of the deception is usually a person or a group of people. But disinformation can also be targeted at a machine. As Clifford Lynch points out in [22], managers of websites sometimes try to fool the automated “crawlers” sent out by search engines to index the Internet. For example, suppose that you have just started selling a product that competes with another product *Y*. When an automated crawler asks for your webpage to add to its index, you might send it a copy of the webpage for product *Y*. That way, when someone uses the search engine to search for product *Y*, the search engine will return a link to your webpage.

4. DISINFORMING = LYING?

Just as Fox began his analysis of information by analyzing the activity of *informing*, this paper begins by analyzing the activity of *disinforming*. In the following section, I will consider the phenomenon of disinformation itself.

A plausible suggestion that philosophers (e.g., [23], p. 231) have made is that disinforming is essentially the same as lying. This equivalence is also suggested by the very title of Russ Kick’s *You Are Being Lied to: The Disinformation Guide to Media Distortion, Historical Whitewashes and Cultural Myths*. In addition, George Carlin’s comment suggests that disinformation is just a euphemism for lying.

This characterization of disinforming is very illuminating and reasonably close to being correct. As noted above, lying often does count as disinforming. But there are several important respects in which lying is not the same as disinforming. These complications need to be considered in order to give a precise analysis of disinforming.

4.1 Intending to Deceive

To begin with, there are a couple of respects in which disinforming is a more restrictive concept than lying. That is, it is

⁴ Similarly, in George Orwell’s *Nineteen Eighty-Four*, functionaries in the Ministry of Truth continually altered historical records to insure that the government was always right.

possible to lie without disinforming. First of all, in order to disinform, you have to intend to deceive someone (cf. [2], p. 134, [23], p. 231). But it is possible to lie to someone even if you do not intend to deceive her (cf. [24], p. 289, [25], [26]). For example, suppose that you are guilty of a crime that everyone knows that you committed. However, there is not enough evidence to convict unless you confess. So, you say to the police, “I am innocent,” even though you know that they will not believe you. In this case, you have lied to the police. But you have not disinformed them because you do not intend them to believe something false (i.e., you do not intend to deceive them). As Roy Sorensen points out in [25], such “bald-faced lies do not fool anyone. They are no more a threat to truth telling than sarcastic remarks.”

Of course, most lies are intended to deceive. And these are arguably the most important type of lies. For example, these are the lies that we build lie detectors to detect. In addition, these are the lies that most philosophers (especially moral philosophers) are interested in. In fact, the standard philosophical analysis of lying requires an intention to deceive (cf. [27], section 1.4). James Fetzer probably intended to equate disinforming with such *deceptive lying*.

(D₁) You *disinform* X if and only if:

1. You say that *p* to X.
2. You believe that *p* is false.
3. By saying *p*, you intend X to infer that *p*.

It is worth noting that, while you have to intend to deceive someone, disinforming does not require that she actually ends up being deceived. It is also worth noting that you must intend to deceive and not just intend to disseminate false information. For example, every map is inaccurate to some degree and the cartographer who made the map knows it. If certain features, such as roads, were really drawn to scale, they would be too small to see (cf. [21], p. 30). But despite such inaccuracies, it is clearly not the case that all maps are disinformation. Furthermore, the cartographer is not disinforming people even if they happen to be misled by such features.

4.2 Actual Falsity

However, D₁ is still not restrictive enough. In order to disinform, you have to intend that someone infer something that is actually false. But it is possible to (deceptively) lie to someone even if you intend her to infer something that (unbeknownst to you) is actually true. For example, suppose that the police ask you about your friend Ramon’s whereabouts and that you want to mislead them about where he is. You believe that he is staying with his cousins outside the city. So, you say to the police, “he is hidden in the cemetery.” However, without your knowledge, Ramon has actually hidden himself in the cemetery. In this case, you have lied to the police (cf. [26], [27], section 1.2). But you have not disinformed them because what you intend them to believe is not actually false. It is clear, for example, that librarians are primarily worried about their patrons getting information that actually is inaccurate (cf. [2], p. 134). Thus, it might be suggested that you disinform if you say something that actually is false with the intent to deceive.

(D₂) You *disinform* X if and only if:

1. You say that p to X.
2. You believe that p is false.
3. By saying p , you intend X to infer that p .
4. p is false.

4.3 Communicate Deceptively

However, D_2 is too restrictive. You can disinform someone even if you know that what you are saying is true. In order to disinform, you must intend to bring about a false belief. But the actual information that you provide does not have to be false. For example, suppose that a murderer asks about your friend Joe's whereabouts and that you want to mislead him about where he is (cf. [28], pp. 437-38). You believe that he is hiding in the basement. So, you truthfully say to the murderer, "he's been hanging around the drugstore a lot" intending that the murderer draw the false conclusion that he is at the drugstore now. In this case, you have disinformed the murderer without saying anything that you believe to be false.

Most philosophers think that you are not lying in such a case because you are saying something that you believe to be true (cf. [27], section 1.2). But several people (e.g., [29], [30], [31]) have a broader notion of lying that counts such *false implicatures* (or "half-truths") as lies. These people think that it is the intention to deceive that really determines whether someone is lying. Thus, according to these people, a liar does not have to say something that she believes to be false. She just has to *communicate* something that she believes to be false. Similarly, it might be suggested that you disinform if you *communicate* something false that you believe to be false.

(D_3) You *disinform* X if and only if:

1. You communicate that p to X.
2. You believe that p is false.
3. By communicating p , you intend X to infer that p .
4. p is false.

4.4 Disseminate Misleading Information

However, D_3 is still too restrictive. First, you can only communicate *to* someone. But you can disinform someone without communicating anything directly to him. For example, suppose that you want to trick your friend Benedick into believing that Beatrice is in love with him. So, you say to a companion (who is in on your little scheme) that Beatrice is in love with Benedick when you know that Benedick is eavesdropping on your conversation. In this case, you have disinformed Benedick. In fact, this is the same sort of disinforming that happened with the fake radio transmissions during World War Two. But you have not communicated *to* Benedick that Beatrice is in love with him. In order for you to do this, it would have to be completely *open* between the two of you that you have said that Beatrice is in love with him. In other words, communicating has a *common knowledge* requirement that disinforming does not (cf. [31], section 3).

Second, you can only communicate *that* some state of affairs obtains. In other words, you must be expressing a proposition (e.g., that Beatrice is in love with Benedick). But you can disinform without expressing any particular proposition. For example, you can disinform with a doctored photograph or a

falsified map. Things like photographs and maps do not have *propositional content*. In other words, they are not descriptions of the world that are either true or false. These things only have *representational content*. That is, they can simply be more or less accurate depictions of the world.⁵

But we can easily fix both of these problems with D_3 simply by replacing the communication requirement with the requirement that you simply disseminate some information.

(D_4) You *disinform* X if and only if:

1. You disseminate information i .
2. You believe that p is false.
3. By disseminating information i , you intend X to infer that p .
4. p is false.

Now, to give a full account what it is to disinform, we really need to say exactly what *information* is. And, in fact, there are many different (often conflicting) theories of information to choose from (cf. [3], pp. 39-74). But D_4 arguably provides a useful analysis of disinforming even if we simply assume a common sense understanding of what information is. We just need to stipulate one substantive, and somewhat controversial, thing about the nature of information. Namely, information need not be true or accurate (cf. [3], p. 160, [32]).

While you can disinform by saying something true, in the prototypical cases of disinforming, you say something false. For example, when the President said to the American people, "I did not have sexual relations with that woman, Miss Lewinsky," he seemed to be disseminating *false* information. However, according to several philosophers (e.g., [33], pp. 45-46, [34], pp. 887-90, [35], 360-365), the President did not disseminate any *information* in this case; false or inaccurate information is not information at all. As Fred Dretske puts it in [36], "false information, misinformation, and (grimace!) disinformation are not varieties of information—any more than a decoy duck is a kind of duck." But even for these philosophers, there is a broader category of stuff that encompasses both information and "inaccurate information." Namely, there is stuff with *representational content*. And the term 'information' in D_4 should simply be understood as referring to stuff with representational content.

4.5 Reasonable to be Deceived

However, even once we stipulate that information need not be true, D_4 is still not quite right. Even if you intend to deceive X, you have not disinformed X if it is not reasonable to infer p from the information that you have disseminated. For example, if you say to the murderer, "Joe has been under the weather," intending that he come to believe that Joe is at the drugstore now, you have not disinformed him. In order for you to disinform someone, it has to be reasonable for her to draw the false conclusion that you intend them to draw. In a similar vein, according to the Federal Trade Commission, in order to count as deceptive advertising,

⁵ Even for people who endorse a narrow analysis of lying, lies do not have to be verbal utterances (cf. [27], section 1.1). For example, you can lie by writing a letter or sending smoke signals. But you can disinform without using language at all.

“the representation, omission or practice must be likely to mislead reasonable consumers” (quoted in [37], p. 188).

(D₅) You *disinform* X if and only if:

1. You disseminate information *i*.
2. You believe that *p* is false.
3. You intend X to infer from information *i* that *p*.
4. *p* is false.
5. It is reasonable for X to infer from information *i* that *p*.

More concisely, what is required for disinforming is that you disseminate some information (condition 1) that you intend to be misleading (conditions 2 and 3) and it actually is misleading (conditions 4 and 5).⁶

It is worth noting that condition 5 rules out the articles in *The Onion* as cases of disinforming. These articles are intended to be humorous rather than misleading. But even if the editor of *The Onion* did hope to deceive her audience with a particular article, she would still not be disinforming them. It would not be reasonable for people to infer that “Al Gore Places Infant Son in Rocket to Escape Dying Planet” from the fact that *The Onion* says so.

4.6 Deceptive Content

However, D₅ is still not quite right. The *content* of the information has to play a role in the deception. Otherwise, we are just talking about run-of-the-mill deception. For example, suppose that you truthfully say to King Arthur in a heavy French accent, “we’ve already got a Holy Grail” intending that he draw the false conclusion that you are francophone. In this case, you have certainly attempted to deceive the King (using information), but you have not disinformed him (as long as you do have a Holy Grail). You are no more disinforming him than if you had put on a beret intending that he draw the false conclusion that you are francophone. If such cases counted as disinforming, it would arguably be just another word for deceiving.

(D₆) You *disinform* X if and only if:

1. You disseminate information *i*.
2. You believe that *p* is false.
3. You intend X to infer from the content of information *i* that *p*.
4. *p* is false.
5. It is reasonable for X to infer from the content of information *i* that *p*.

While the content must play a role in the deception, it should be noted that things beyond the content of the information can also play a role. For example, if you create a map of South America to look like it was drawn by Europeans in the 17th century (e.g., on old parchment, with ornate lettering) to try to misled people into thinking that Machu Picchu was discovered in the 17th century, you would seem to be disinforming these people.

4.7 Deception Foreseen

However, it is possible that D₆ is still not quite right. There are cases where people spread “deliberately misleading information” but do not intend to deceive anyone by doing so. In fact, in at least two of our examples of disinformation, it is not clear that the perpetrator really intended to deceive anyone. For example, the person who modified the Seigenthaler entry on Wikipedia claimed that he was just playing a joke on a friend. Also, the hacker who modified the *Yahoo! News* website apparently did so in order to alert people to the security vulnerabilities of the website.

Now, it might be suggested that, in these cases, the perpetrator really did intend to deceive. For example, the joke would not have been funny (maybe it was not funny anyway) if the friend had not been taken in. In other words, deception was a necessary means to the ultimate goal of the perpetrator. Also, if the hacker had really not wanted to deceive anybody, he could have exposed the security problem by simply vandalizing the *Yahoo! News* website rather than by posting a false news story.

But there are other examples of “deliberately misleading information” where there is very clearly no intention to deceive. For example, many cartographers deliberately falsify their maps. In order to protect their intellectual property, many cartographers add a few features to their maps that do not really exist in the world (cf. [21], pp. 49-51). If these non-existent features show up in another map of the same area, the cartographer has good evidence that her work has been copied. But these cartographers do not intend to mislead map users about these non-existent features.

Also, people have intentionally placed inaccurate information on the Internet for educational purposes (cf. [38], [39], p. 10). For example, a website for the *Oklahoma Association of Wine Producers* and a website advertising a town in Minnesota as a tropical paradise were created to teach people how to identify inaccurate information on the Internet. In fact, people (e.g., [2]) have intentionally placed inaccurate information on the Internet for research purposes as well. For example, several researchers have put false information into Wikipedia to see how long it takes to get corrected (cf. [7], p. 1665).

In all of these cases, the perpetrator has some goal other than deception that she is trying to achieve (such as teaching people how to evaluate websites or protecting her intellectual property). And she may be able to achieve this other goal even if no one is deceived. In addition, this other goal may often be sufficiently laudable that it provides an *excuse* for having deceived someone. But it is important to note that having an excuse for having deceived someone does not mean that the perpetrator has not disinformed him.

While disinforming may not require that the source of the misleading information intend to deceive people, it does at least require that the source of the information *foresee* that people will be deceived.⁷ In other words, unlike lying, disinforming is always

⁶ Condition 5 just makes explicit something that is implicit in any analysis of lying. For example, it goes without saying that, if you communicate *p*, then it is reasonable for someone to infer that *p*.

⁷ Philosophers draw a distinction between (a) what a person intends to do by performing an action and (b) what a person simply foresees as a likely “side effect” of performing that action (cf. [24], p. 291). But there is a debate over whether this

about deception at some level. For example, the cartographers know that some map users might end up believing that these non-existent streets really exist. Similarly, the hacker had to foresee that some people might end up believing his false news story. So, what we may need to say is that you disinform if you believe that your information is *misleading*.⁸

(D₇) You *disinform* X if and only if:

1. You disseminate information *i*.
2. You believe that *p* is false.
3. You foresee that X is likely to infer from the content of information *i* that *p*.
4. *p* is false.
5. It is reasonable for X to infer from the content of information *i* that *p*.

Even if they do not intend to fool anybody, I am sure that the editors of *The Onion* can predict that they are going to fool at least a few people. In fact, I hear many people say that, the first time that they read *The Onion*, they thought that it was for real. But the editors of *The Onion* are not disinforming their audience because it is not reasonable to infer *p* from the fact *The Onion* says *p*. Even those people who are deceived initially are usually not deceived for very long. So, the information on *The Onion* still does not count as disinformation under D₇.

4.8 Very Close to Lying

If we understand deceptive lying in a sufficiently broad sense, disinforming is very close to deceptive lying. However, it is worth noting that disinforming (whether we adopt D₆ or D₇) does not include all deceptive behavior. For example, it excludes certain parts of the disinformation campaign used by the Allies during World War Two. In addition to sending fake radio transmissions, the Allies built fake tanks and airplanes out of rubber and canvas to give the false impression that a huge force was preparing to attack Calais. In this case, the Allies were not disinforming because they were not disseminating any information.

Admittedly, we could weaken the analysis of disinforming to include such cases. But then all deceptive behavior would count as disinforming. In that case, we would not really need a separate term for the concept. Also, it would not be a concept of specific interest to information science.

5. DISINFORMATION

Now that we understand the activity of disinforming, it is time to look at what disinformation itself is. But this is pretty

distinction has any moral importance. The debate here between D₆ and D₇ is over whether this distinction has any ontological significance with regard to whether an action counts as an instance of disinforming.

⁸ If you *should have known* that X would be misled by the information that you disseminated, you may very well be morally culpable. But if you are sincerely surprised when X is actually misled, it still seems like an honest mistake on your part. In other words, it is probably not sufficient for disinforming that it be reasonable for you to think that X is likely to be misled. You have to at least foresee that X is likely to be misled.

straightforward. There is a clear-cut “linking principle” between the activity of disinforming and the phenomenon of disinformation (cf. [3], pp. 187-91). Namely, disinformation is the information (i.e., the stuff with representational content) disseminated by someone who is disinforming. Plugging the proposed analysis of disinforming from the preceding section into this principle, disinformation turns out to be misleading information that is intended to be (or at least foreseen to be) misleading.

But there is at least one important complication that should be noted. Disinformation does not have to come *directly* from someone who disinforms. Something is still disinformation even if it has been innocently passed on to me by a friend, a librarian, or a reporter. For example, when news services repeated the fraudulent press release about the Emulex Corporation, they were certainly passing along disinformation. But unlike the creator of this fraudulent press release, the news services themselves were not disinforming the public. They were only misinforming them.

In order for something to count as disinformation, it clearly does not have to be the *immediate* source of the information who believes that the information is misleading. In addition, it may not have to be the *original* source who believes that the information is misleading. Information often passes through many hands before it reaches the end user. It may be enough that one of these intermediaries believes that the information is misleading. In the case of the historical fabrications discussed by Sowards in [13], the original authors undoubtedly foresaw that the information was misleading. Thus, such historical fabrications certainly count as disinformation. However, in other cases, even if the original authors believed that the information was accurate, other people may come along later and spread the same information further with the intent to deceive.

In fact, we might even want to consider out-of-date medical information in the library to be disinformation (cf. [40], p. 83). While the original authors of an old medical textbook may have been completely sincere, the librarian may foresee that he is passing along information that is likely to mislead some patrons. Thus, at least if we adopt D₇ as our analysis of disinforming, such a case would count as disinformation.⁹

Finally, it is also worth emphasizing that, while disinformation will typically be inaccurate, it does not have to be inaccurate. It just has to be misleading. So, disinformation is actually not a proper subset of inaccurate information.

6. APPLICATIONS OF THE ANALYSIS

As noted in the introduction, information scientists are confronted with several important questions about disinformation. In this final section, I briefly gesture at how the foregoing analysis of disinformation might be used to help answer a couple of these

⁹ If the librarian puts the old medical textbook in the reference collection, it definitely seems like disinformation. But if the librarian puts the textbook in the main collection, it may not be disinformation because it is not reasonable for the patron to conclude that what the textbook says is true. After all, libraries collect many books for their historical value rather than for their accuracy.

questions. Most notably, because our conceptual analysis indicates that disinforming is very close to deceptive lying, we can often leverage existing research on lying.

6.1 The Prevalence of Disinformation

First, a greater understanding of what disinformation is can potentially help us to determine how big of a problem disinformation really is and where the problem lies. According to many people (e.g., [41]), disinformation is everywhere. But such a conclusion is largely based on anecdotal evidence. Empirical studies (e.g., [42]) have looked at how much inaccurate information is on the Internet. But these studies have not looked specifically at how much of this inaccurate information is “deliberately misleading.” Even in the absence of an empirical study, however, we can potentially use game theory to predict how prevalent disinformation will be in particular contexts.

Elliot Sober has constructed a game theoretic model of deceptive lying in [43]. Since disinforming is very close to deceptive lying, Sober’s model can arguably be applied to disinforming as well.¹⁰ According to this model, whether a person will disinform depends on the expected costs and benefits. In particular, it depends on the costs of not being believed (weighted by the probability that this will happen) as compared with the benefits of being believed (weighted by the probability that this will happen). Thus, there will be a lot of disinformation if the benefits of being believed are high relative to the costs of not being believed and/or if the intended audience of the disinformation is much more likely to be credulous than to be skeptical.¹¹

We can use this model to account for the prevalence of disinformation in certain contexts. For example, this model arguably explains why we might expect a lot of half-truths and outright lies in an election campaign. There are significant benefits to being believed (in particular, by swing voters) and not much downside if you are caught lying (because the people who would be most incensed would not have voted for you any way).

6.2 The Identification of Disinformation

Second, a greater understanding of what disinformation is can potentially help us to identify disinformation so that people can avoid being misled by it. In the previous sections, I described the properties that a piece of information must have in order to count as disinformation. But it is no simple matter to determine whether a particular piece of information actually has those properties.

Since disinforming is very close to lying, a lot of the vast research on lie detection can potentially be applied to disinformation detection. Researchers in lie detection have focused primarily on *physiological* indicators of deception, such as perspiration and high pulse rate (cf. [29], pp. 51-52). However, we do not always

¹⁰ Understanding exactly how disinforming differs from lying may suggest ways to refine this model.

¹¹ Whether the intended audience is more likely to be credulous or to be skeptical depends on *their* cost-benefit analysis. In particular, will the benefits of acquiring a true belief (weighted by the probability that this will happen) outweigh the costs of acquiring a false belief (weighted by the probability that this will happen)?

come into direct physical contact with sources of disinformation. And even if we do come into direct physical contact, we are rarely in a position to give this source a polygraph test. But techniques have also been developed that can be used to identify lies in recorded information. For example, researchers have used textual analysis to find that liars are somewhat less likely to use first-person pronouns (cf. [44]).¹²

7. REFERENCES

- [1] Fox, C., Levitin, A. and Redman, T. 1994. The notion of data and its quality dimensions. *Information Processing and Management* 30, 9-19.
- [2] Hernon, P. 1995. Disinformation and misinformation through the internet: Findings of an exploratory study. *Government Information Quarterly* 12, 133-139.
- [3] Fox, C.J. 1983. Information and misinformation. Greenwood Press, Westport, Connecticut.
- [4] Farquhar, M. 2005. A treasury of deception. Penguin, New York.
- [5] Fowler, B., Franklin, C. and Hyde, R. 2001. Internet securities fraud: Old trick, new medium. *Duke Law and Technology Review*
DOI=<http://www.law.duke.edu/journals/dltr/ARTICLES/2001dltr0006.html>
- [6] Farid, H. 2008. Digital image forensics. *Scientific American* 298, 66-71.
- [7] Fallis, D. 2008. Toward an epistemology of Wikipedia. *Journal of the American Society for Information Science and Technology* 59, 1662-1674.
- [8] Johns, A. 1998. The nature of the book. University of Chicago, Chicago.
- [9] Floridi, L. 1996. Brave.Net.World: The Internet as a disinformation superhighway? *The Electronic Library* 14, 509-514.
- [10] Tadjman, M. and Mikelic, N. 2003. Information science: Science about information, misinformation and disinformation. *Proceedings of Informing Science + Information Technology Education*, 1513-1527.
- [11] Stahl, B.C. 2006. On the difference or equality of information, misinformation, and disinformation: A critical research perspective. *Informing Science* 9, 83-96.
- [12] Gackowski, Z.J. 2006. Quality of informing: Bias and disinformation, Philosophical background and roots. *Issues in Informing Science and Information Technology* 3, 731-744.
- [13] Sowards, S.W. 1988. Historical fabrications in library collections. *Collection Management* 10, 81-88.
- [14] Council of the American Library Association. 2005. Resolution on disinformation, media manipulation & the destruction of public information.
DOI=<http://www.ala.org/ala/ourassociation/governance/council/councilagendas/annual2005a/CD64.doc>

¹² We can also look for indicators of sincerity to determine that a piece of information is not disinformation. These need to be things that it is difficult for deceivers to fake (cf. [45], p. 474).

- [15] Margolis, E. and Laurence, S. 2006. Concepts. *Stanford Encyclopedia of Philosophy*
DOI=<http://plato.stanford.edu/entries/concepts/>
- [16] Austin, J.L. 1956. A plea for excuses. *Proceedings of the Aristotelian Society* 57, 1-30.
- [17] Steup, M. 2001. The analysis of knowledge. *Stanford Encyclopedia of Philosophy*
DOI=<http://plato.stanford.edu/entries/knowledge-analysis/>
- [18] The Smoking Gun. 2006. A million little lies. *The Smoking Gun*
DOI=<http://www.thesmokinggun.com/archive/0104061jamesfrey1.html>
- [19] Fleischer, M. 2006. Navahoax. *LA Weekly*
DOI=<http://www.laweekly.com/general/features/navahoax/12468/>
- [20] Fiore, F. and Francois, J. 2002. Disinformation – Changing web site contents.
DOI=<http://www.informit.com/articles/article.aspx?p=29255>
- [21] Monmonier, M. 1991. How to lie with maps. University of Chicago, Chicago.
- [22] Lynch, C.A. 2001. When documents deceive: Trust and provenance as new factors for information retrieval in a tangled web. *Journal of the American Society for Information Science and Technology* 52, 12-17.
- [23] Fetzer, J.H. 2004. Disinformation: The use of false information. *Minds and Machines* 14, 231-240.
- [24] Carson, T.L. 2006. The definition of lying. *Nous* 40, 284-306.
- [25] Sorensen, R. 2007. Bald-faced lies! Lying without the intent to deceive. *Pacific Philosophical Quarterly* 88, 251-264.
- [26] Fallis, D. 2008. What is lying?
DOI=<http://dlist.sir.arizona.edu/2100/>
- [27] Mahon, J. 2008. The definition of lying and deception. *Stanford Encyclopedia of Philosophy*
DOI=<http://plato.stanford.edu/entries/lying-definition/>
- [28] Adler, J.E. 1997. Lying, deceiving, or falsely implicating. *Journal of Philosophy* 94, 435-452.
- [29] Ekman, P. 1985. Telling lies. W. W. Norton, New York.
- [30] Simpson, D. 1992. Lying, liars and language. *Philosophy and Phenomenological Research* 52, 623-639.
- [31] O'Neill, B. 2003. A formal system for understanding lies and deceit.
DOI=<http://www.sscnet.ucla.edu/polisci/faculty/boneill/bibjerr5.pdf>
- [32] Fetzer, J.H. 2004. Information: Does it have to be true? *Minds and Machines* 14, 223-229.
- [33] Dretske, F.I. 1981. Knowledge & the flow of information. MIT Press, Cambridge.
- [34] Frické, M. 1997. Information using likeness measures. *Journal of the American Society for Information Science* 48, 882-892.
- [35] Floridi, L. 2005. Is information meaningful data? *Philosophy and Phenomenological Research* 70, 351-370.
- [36] Dretske, F.I. 1983. Précis of Knowledge and the flow of information. *Behavioral and Brain Sciences* 6, 55-90.
- [37] Carson, T.L. 2002. Ethical issues in selling and advertising. In *The Blackwell Guide to business ethics*, N.E. Bowie, Ed. Blackwell, Malden, Massachusetts, 186-205.
- [38] Piper, P.S. 2000. Better read that again: Web hoaxes and misinformation. *Searcher* 8,
DOI=<http://www.infotoday.com/searcher/sep00/piper.htm>
- [39] Wachbroit, R. 2000. Reliance and reliability: The problem of information on the Internet. *Report from the Institute for Philosophy & Public Policy* 20, 9-15.
- [40] Pendergrast, M. 1988. In praise of labeling; or, when shalt thou break commandments? *Library Journal* 113, 83-85.
- [41] Kick, R. 2001. You are being lied to: The disinformation guide to media distortion, historical whitewashes and cultural myths. Disinformation Company, New York.
- [42] Impicciatore, P., Pandolfini, C., Casella, N. and Bonati, M. 1997. Reliability of health information for the public on the world wide web: Systematic survey of advice on managing fever in children at home. *British medical journal* 314, 1875-1879.
- [43] Sober, E. 1994. The primacy of truth-telling and the evolution of lying. In *From a biological point of view*, Cambridge, Cambridge, 71-92.
- [44] Newman, M.L., Pennebaker, J.W., Berry, D.S. and Richards, J.M. 2003. Lying words: Predicting deception from linguistic styles. *Personality and Social Psychology Bulletin* 29, 665-675.
- [45] Fallis, D. 2004. On verifying the accuracy of information: Philosophical perspectives. *Library Trends* 52, 463-487.